Governor Janet Napolitano

ADOA/ISD/AIS
Monthly Cyber Security Tips
NEWSLETTER

May 2008 Volume 3, Issue 5

Using Encryption to Protect Data

ADOA Information Security

AIS Managing Our Information Safeguards

With major data breaches being reported all too frequently, organizations are now placing increased emphasis on security of personal, private and sensitive information. One method of increasing security is through data encryption. Encryption is the process of scrambling a message or data so that no one but the sender and the intended recipient can read it. Militaries, businesses, and governments all over the world use it in a variety of ways.

There are two general types of encryption used for cyber security: hardware-based and software-based. Hardware-based encryption is built into a piece of hardware. An example of hardware-based encryption would be the pre-encrypted hard drives that are currently on the market. All data stored on them is automatically encrypted, even the temporary files. A pre-encrypted USB drive is another example of hardware-based encryption. Software-based encryption refers to an encryption program installed on a computer or a server that encrypts either some or all of the data on the system.

With the increasing use of computers in every aspect of our life, and the need to protect the information on those computers, the use of encryption has expanded. Here are some examples of where encryption can be a key component of a defense-in-depth strategy:

- **Laptop protection** - The first use for encryption many people think of is encrypting the data on laptops. This can be done by encrypting specific directories and files or by encrypting the entire hard drive (full disk encryption). Some analysts recommend using both forms of encryption on the same laptop as that is more secure than either method on its own. Minimally, file level encryption should be implemented; full disk encryption is a best practice.

- **Wireless networks** –Confidential and valuable data can be intercepted by hackers while being transmitted over wireless networks unless appropriate encryption is employed. Most wireless networks extend out far past the walls of the building where they are located. Anyone in the parking lot or on a nearby street may be able to access the wireless network. In order to prevent unauthorized access, wireless networks need to be configured to employ the appropriate encryption methodology. *(See the February 2008 Wireless Security Monthly Security Tips Newsletter for more information.)*

- **Email and Instant Messaging (IM)** – It is important to realize that email and IM messages hit numerous servers and routers before reaching their final destination. They can be intercepted at any stage in this journey and if they are not encrypted, the data is vulnerable to being accessed. Therefore, no confidential or sensitive data should be sent via email in clear text or

transmitted via Instant Messaging.

- **Backup tapes and media** – Many cases of data breach have been the result of backup tapes and other storage media being lost or stolen. These items should be encrypted to prevent unauthorized access.

- **Removable Media** – CDs, DVDs, and USB flash drives are all capable of holding large amounts of data, and these removable devices are being used more frequently. However, one must be vigilant about where these devices are used and the potential vulnerabilities of using them on an unprotected system. These devices should be encrypted. You can also purchase pre-encrypted USB drives.

- **Smartphones, PDAs and other similar devices** – These devices can hold a large amount of data. Because of their small size, they can more easily be lost or stolen, putting the data on them at risk. Where practicable, these devices should be encrypted.

There are a variety of encryption tools available in the marketplace—some of which are open source--however, please note any solution you implement should be compliant with accepted industry standards. Given the current technology environment, you should minimally employ a 128-bit Advanced Encryption Standard (AES) solution.

For more information on encryption visit the following:

Protecting Portable Devices www.msisac.org/awareness/news/2007-02.cfm
Securing a Wireless Network www.msisac.org/awareness/news/2008-02.cfm
Understanding Encryption www.us-cert.gov/cas/tips/ST04-019.html
Overview of Encryption: www.cescomm.co.nz/industry.html
Encryption Tutorial: www.webmonkey.com/programming/php/tutorials/tutorial1.html

For more cyber security monthly tips go to: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's cyber security posture.

Brought to you by:

MS-ISAC

www.msisac.org